



DEPARTMENT OF THE AIR FORCE AIR EDUCATION AND TRAINING COMMAND

NOTE: This document provides information about the law designed to help you safely cope with your own legal needs. But legal information is not the same as legal advice -- the application of law to an individual's specific circumstances. Although we go to great lengths to make sure our information is accurate and useful, we recommend you consult a lawyer if you want professional assurance that our information, and your interpretation of it, is appropriate to your particular situation

Identity Theft

Identity theft occurs when someone uses your personal information without your permission to commit fraud or other crimes. An identity thief may use your information to obtain new credit cards, open checking accounts, obtain a driver's license or Social Security card, make long distance calls, apply for a job, or make purchases using your name and your bank account or credit card.

Identity theft is a felony crime, but because of the nature of the crime, you may not realize your identity has been stolen until you are denied credit, turned down for a job, or sent a bill for purchases you did not make. By that time, your good name and credit history may be in ruins. Rebuilding good credit in the aftermath of identity theft can take months - or even years.

While you can't entirely control whether you will become a victim, there are steps you can take to minimize your risk. As such, all veterans need to be extra vigilant and to carefully monitor bank statements, credit card statements, and any statements relating to recent financial transactions for unusual or suspicious activity.

Suspicious activities could include the following:

- You receive bills from a credit account you did not open.
- You notice purchases or charges on your credit, long distance phone, or bank accounts that you did not make.
- Unauthorized changes are made to existing authorized charge accounts.
- Companies you have not contacted or done business with or a collection agency inquires about a debt you did not incur.
- Bank, credit billing statements, and other bills do not arrive as expected.
- You receive unexpected credit cards or account statements.

- You are turned down for a credit card, loan, mortgage, or other form of credit due to unauthorized debts on your credit report.
- You are denied credit for no apparent reason.
- Your credit report shows accounts you did not authorize.
- If you notice unusual or suspicious activity, you should take the following steps:

Step 1 – Contact the fraud department at all of the three major credit bureaus:

- Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
- Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, Texas 75013
- TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

The credit bureaus will send copies of your credit reports so you may review the credit reports carefully to make sure no additional fraudulent accounts were opened in your name or unauthorized changes made to existing accounts. You should also request that the credit reporting agencies place a fraud alert in the file, as well as a victim's statement asking that creditors call before opening any new accounts or changing existing accounts. A fraud alert may delay, interfere with or prohibit the timely approval of any subsequent request or application a consumer would make that involves access to their credit report, to include new loan, insurance, obtaining rental property, employment, and other transactions that require access to a consumer's credit report.

Additionally, while a consumer's report is frozen, companies that provide consumer data to the credit reporting bureaus will not be allowed to update name and address information on a consumer's report. The consumer must do this directly with the credit reporting bureau. A fraud alert lasts for at least 90 days and can be extended for up to 7 years by written request and by providing a copy of an identity theft report.

Twenty-three (23) states have passed "security freeze" laws that allow consumers to indefinitely prevent anyone from issuing credit in their name. These states include, California, Colorado, Connecticut, Florida, Illinois, Kentucky, Louisiana, Maine, Minnesota, Nevada, New Hampshire, New Jersey, New York, North Carolina, Oklahoma, Utah, Vermont and Wisconsin. Hawaii, Kansas, South Dakota, Texas and Washington only provide that identity theft victims may place a "security freeze" to prevent someone from opening credit in their name.

Step 2 – Close any accounts that have been tampered with or opened fraudulently.

Step 3 – File a police report with your local police or the police in the community where the identity theft took place. Get a copy of the report or at the very least, the number of the report, to submit to your creditors and others that may require proof of the crime.

Step 4 – File a complaint with the Federal Trade Commission by using the FTC's Identity Theft Hotline:

- By telephone: 1-877-438-4338
- Online at www.consumer.gov/idtheft
- By mail at: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington DC 20580.

The Department of Veterans Affairs has established a dedicated toll free telephone number (1-800-FED-INFO) for questions or concerns connected with this loss of data. You can also visit their website at www.firstgov.gov for updates.